

Key Findings of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

PRE-BOMBING

- Government agencies were in possession of significant pieces of information that, taken together, would have led a competent analyst to conclude that Flight 182 was at high risk of being bombed by known Sikh terrorists in June 1985.
- James Bartleman's evidence that, shortly before the bombing, he saw a specific threat to Air India Flight 182, is credible. The Commission accepts the possibility that such a document would have been ignored and then subsequently have gone missing.
- Additional, highly classified, threat information was in the possession of the Communications Security Establishment (CSE). This information, which was received by the Commission after the close of the hearings, was consistent with other information about the threat of sabotage and hijacking by Sikh extremists in June 1985, and indicated that Indian airports were undertaking security audits in response to the threat.
- Even without the evidence of James Bartleman and the CSE information, the Commission finds that the amount of information collectively held by the Government made the failure to implement appropriate anti-sabotage measures inexcusable.
- The view of Canadian officials prior to the bombing that government-owned Air India was "crying wolf" in order to obtain additional security for free was misguided.
- The institutional arrangements and practices of information-gathering agencies were wholly deficient in terms of internal and external sharing of information, as well as analysis.
- Government agencies failed to appreciate the nature and the seriousness of the threat of Sikh extremism.
- The five-month delay in CSIS' application to intercept Parmar's communications, which was a result of a warrant conversion process that prioritized existing warrants over new applications, was entirely disproportionate to the level of the threat.
- CSIS surveillance was ineffective. Surveillants were unable to distinguish one traditionally attired Sikh from another. When a CSIS surveillance team observed experiments involving a test explosion conducted by Sikh extremists in the woods in Duncan B.C. in June 1985 (the Duncan Blast), the loud sound heard was misinterpreted as a gunshot. No photograph was taken of the unknown third person present (Mr. X.) because surveillants had not brought a camera.

- CSIS failed to include important information, such as the Duncan Blast, in the threat assessments it provided to the RCMP and Transport Canada.
- The RCMP wasted resources creating a threat assessment structure parallel to CSIS'. The RCMP structure was itself ineffective - it failed to identify, report, and share threat information.
- The RCMP failed to transmit the June 1st Telex, warning about the possibility of bombing with time-delayed devices in June 1985, to either CSIS or to Transport Canada.
- Excessive secrecy in information sharing prevented any one agency from obtaining all necessary information to assess the threat. Excessive secrecy also prevented those on the frontlines from obtaining information necessary to put in place security measures responsive to the threat.
- Effective protective measures were not implemented in response to the threat to Air India Flight 182.
- The concept of "specific threat" was misunderstood and misapplied. When a call-in bomb threat was deemed to be "specific," it would trigger an elaborate airport emergency protocol which, had it been employed on June 22, 1985, would likely have identified the bomb. This protocol had no application outside of the call-in threat situation. When intelligence was received through other channels, a lack of extreme specificity was at times wrongly used to deny additional protective resources.
- Today, the concept of specific threat has become an excuse to explain why more was not done to prevent the bombing on June 22, 1985.
- Security measures in response to possible threats to aviation were poorly thought out and mechanically applied. They were not tailored to meet the particular nature of the threat.
- Despite the knowledge of the threat of sabotage, Transport Canada and RCMP Protective Policing displayed a lack of flexibility by continuing to rely on anti-hijacking security measures, which did not address the threat of bombing.
- There was a lack of cooperation and communication within the RCMP and between RCMP, Transport Canada and airlines in relation to airport security.
- Although Air India was operating under an elevated threat level, CP Air (the airline upon which the bomb was loaded in Vancouver) was not informed of this fact and was operating under normal security protocols.

- In retrospect, the behaviour of those who booked and paid for the tickets and checked-in the bags should have raised red flags, but a customer service mentality governed at the time, and airline staff were not instructed to watch for indicia of harmful intentions.
- In allowing the unaccompanied bag to be loaded on to its Toronto-destined flight, CP Air failed to follow its own baggage security procedures.
- Transport Canada failed to pass then existing draft regulations, which would have enhanced the security of Canadian airports, and failed until after the bombing to implement known anti-sabotage measures.
- One anti-sabotage measure known at the time was passenger-baggage reconciliation (a process of matching passengers with their baggage in order to prevent unauthorized bags from being placed on board aircraft, treating the passenger and their baggage as a single entity). Had passenger-baggage reconciliation been used, the bombing of Air India Flight 182 would have been prevented.
- Canadian airports were plagued by a lax security culture. Restricted areas were not adequately protected, and private security guards and janitorial staff were not required to undergo criminal record checks. Persons with known associations to Sikh extremist groups had access to highly sensitive areas at Vancouver International Airport.
- Privatization and cutbacks had a negative impact on airport security. Air India was left to implement security measures with little to no supervision by Government. Personnel in charge of screening the luggage, who were employees of a private security company, were underpaid and inadequately trained.
- At Pearson airport, RCMP and Transport employees were aware of ongoing problems with the X-ray machine and had demonstrated the PD4 sniffer to be ineffective. On the day of the bombing, the remaining bags were scanned only with the PD4 sniffer when the X-ray machine failed. The security employees contracted by Air India had no prior experience or formal training in the operation of the PD4. No one informed the supervisors that the device may have reacted to some of the bags it scanned.
- Air India ought to have known that the security measures it was using were inadequate to prevent a bomb being placed on its aircraft.
- On June 22, 1985, the security level in force at Pearson and Mirabel airports called for the use of an RCMP explosives detection dog (EDD). That weekend, however, all RCMP EDD teams were in Vancouver for training, leaving the Toronto airport without any coverage.

- On the day of the bombing, Mr. Brian Simpson, an Air Canada summer employee at the time, was able to board the Air India aircraft stationed outside the international departures area of Pearson, walk around for 10 minutes or so, and leave, without challenge.
- In Montreal, after three suspicious bags were identified and left unattended, the flight was cleared for departure by Air India before the arrival of the explosives detection dog. Security employee Daniel Lalonde overheard the Air India security officer mention cost-related reasons for this decision.

POST-BOMBING

- CSIS often failed to disclose promptly to the RCMP information relevant to the criminal investigation, particularly information from human sources, or it disclosed information without sufficient detail or in a manner that prevented the RCMP from using the information.
- CSIS was mesmerized by the mantra that “CSIS doesn’t collect evidence,” and used it to justify the destruction of raw material and information. CSIS erased the tapes that caught coded conversations possibly related to the planning of the bombing, and CSIS investigators destroyed their notes that recorded the information CSIS sources provided in relation to the Air India bombing. Both of these actions compromised the prosecution’s evidentiary position at trial.
- CSIS delayed disclosure of necessary information for the prosecution of Interjit Singh Reyat by adopting a legalistic and technical approach in responding to requests from prosecutor James Jardine.
- The RCMP never made a written request that the Parmar tapes be preserved, though it was aware of their existence, and also never made a verbal request specific to the Parmar tapes until months into the investigation, when the early tapes were already erased. CSIS only ceased ongoing erasure in 1986, following a request by the Department of Justice in connection with the civil litigation.
- It is impossible to determine what information, if any, was lost due to the tape erasures and it is impossible to tell whether all tapes were listened to before being erased.
- The RCMP often prematurely discounted or failed to follow up on intelligence leads that did not conform to its primary theory of the case. For example, one suspect was ruled out based on observations, made two years after the bombing, that his hair did not look like the hair of one of the individuals who had checked in the luggage, as depicted in an imprecise composite drawing.
- The RCMP also prematurely dismissed information on the basis of preliminary assessments of credibility. When Person 1, prior to the bombing, provided information about a plot to bomb an

Air India plane, his information was discounted as it was believed he was providing the information for his own personal interests. This suspicion persisted after the bombing and it took months – and critical media reports – before the RCMP reluctantly followed up on Person 1's information, which was ultimately verified by a polygraph examination.

- The RCMP failed to appreciate the continuing threat of Sikh extremism or the fear sources had of their cooperation with the police being discovered. As a result, the RCMP often alienated sources, including sources who had previously been willing to speak to CSIS, because of the manner in which it treated them.
- The RCMP failed to appropriately protect sources and witnesses.
- The RCMP, at times, failed to take threats against Tara Singh Hayer seriously.
- The RCMP eventually installed a video surveillance system in Mr. Hayer's home, after his name appeared on a "hit list." However the system was deficient and was not functioning properly on the day of his murder. The RCMP failed to inform Mr. Hayer's family that no image had been captured on the video cassette.
- The RCMP devoted diminishing resources to the Air India investigation over time, and at one point only one member was assigned to the case.
- The RCMP investigation was plagued by internal strife within the E Division team and between E Division and Headquarters. Creative approaches to the investigation were often discouraged. Little progress was made until the 1995 decision to review and revive the investigation, in part because of a concern about the political fallout of a public admission that the investigation was at an impasse.

OVERALL GOVERNMENT RESPONSE TO THE AIR INDIA BOMBING AND TREATMENT OF THE FAMILIES

- Immediately after the bombing, the Government issued public statements denying any mistakes.
- Early on, officials from Foreign Affairs made sincere efforts to provide assistance to the families, in Canada and in Ireland, with limited resources and without the benefit of formal guidelines, given the unprecedented nature of the disaster.
- During initial inquiries in Ireland and India, instructions were issued to avoid acknowledgement that the crash was caused by a bomb.
- Efforts were made to limit funds expended to respond to the concerns of the families. The civil suit they launched was settled early on by hard bargaining, before disclosure was made of much of the information now learned in this Inquiry.

- The families were not kept informed about the investigation by the Government, and often learned about new developments through the media. The RCMP only began to liaise with the families directly after 1995. CSIS refused to participate.
- Over the past 25 years, the RCMP has at times inappropriately invoked concerns about its ongoing investigation in order to limit the information provided to the families or to external reviewers.
- Government agencies consistently opposed external review and attempted, at times successfully, to avoid or delay such reviews. Concerns about possible prejudice to the Government's position in the civil litigation with the families was cited as one of the reasons for this opposition.
- When a review did proceed in the early 1990s, the agencies coordinated their responses in an attempt to avoid contradiction and present a picture of greater cooperation than in fact existed. The RCMP briefing provided in this review was less than accurate in its description of the ongoing relationship with CSIS.
- The briefings provided by the agencies for the Rae review contained several significant inaccuracies which were not revealed until this Inquiry, including a statement by the RCMP that it had passed on the June 1st Telex to CSIS; a statement by RCMP and Transport that the presence of a dogmaster was part of the security measures in place at Toronto airport on the day of the bombing; and a statement by CSIS that it had advised the RCMP the day after the crash about the CSIS intercept on Parmar's communications.
- The Government over-redacted the documents initially provided for public release in this Inquiry.
- The RCMP inappropriately relied on the fact of its ongoing investigation to deny the Commission important information when it failed, without reasonable justification, to advise the Commission forthwith that an individual who might potentially have had relevant information had requested to speak to the Commission. The RCMP then continued to withhold this information, without justification, even after the usefulness of the individual to the criminal investigation had been discounted.
- The Government had only one set of counsel represent all potentially affected departments and agencies before this Inquiry. This Government decision to "speak with one voice," despite known differences in viewpoint, meant that the Commission was not always presented with a clear statement of the agencies' positions about contentious issues.

THE RELATIONSHIP BETWEEN INTELLIGENCE AND EVIDENCE AND THE CHALLENGES OF TERRORISM PROSECUTIONS

- There is a lack of institutionalized co-ordination and direction in national security matters. Canadian agencies have developed a culture of managing information in a manner designed to protect their individual institutional interests.
- The current practice of attempting to limit the information CSIS provides to the RCMP in order to prevent its disclosure in potential criminal proceedings is misguided, as disclosure obligations at trial are engaged by potential relevance, not by which agency has seen the information. The result of such efforts to deny intelligence to the police is an impoverished response to terrorist threats.
- The processes and procedures by which decisions are made as to what information should be passed exchanged between the intelligence and law enforcement communities are seriously flawed and require substantial revision.
- There is no “silver bullet” solution to reconciling the needs of intelligence and law enforcement. Neither interest is absolute and neither one can trump the claims of the other in all situations. Reform must be directed at improving decision making by ensuring that the decision maker is capable of taking into account both sets of interests as well as the broad national interest. The recommendations are structured to meet that objective.

AVIATION SECURITY

- Many of the same deficiencies in aviation security that were identified in 1985 continue to be raised as urgent concerns today.
- Aviation security is a core governmental function related to national security.
- In aviation security, there is a tendency to focus on “fighting the last war” instead of taking necessary, proactive measures.
- A holistic approach to aviation security is required because terrorists continuously probe aviation security regimes, looking for weaknesses. This approach involves multiple, mutually reinforcing layers of security measures.
- A culture of security awareness accepted by all stakeholders is essential to guard against complacency.
- Air terminals can themselves be target-rich environments for terrorists.
- While fortress-like security is applied to the more publicly visible side of civil aviation, the side that is more hidden from public scrutiny remains exposed.

- Air cargo is neither routinely searched prior to loading, nor subjected to adequate screening measures. Its vulnerability, which has been understood by the Government for decades, makes it a serious potential target for sabotage. Canada does not meet its international treaty obligation to prevent unauthorized explosives and other dangerous devices or substances from being placed on board civil aviation aircraft “by any means whatsoever”. The Government’s failure to take swift action to close this gap is inexcusable.
- Access to airside and restricted areas of airports is poorly controlled and the system for screening non-passengers who access restricted areas of airports can be easily circumvented. Lax perimeter security also allows vehicles and their occupants to enter airside portions of the airport with minimal, if any, screening. As a result, aircraft and passengers are vulnerable to attack.
- CATSA has encountered significant difficulties in recruiting and retaining screening personnel.
- Behavioural analysis (direct observation of passengers prior to boarding aircraft) is already being conducted in airports and on some flights by Aircraft Protection Officers (RCMP officers assigned to Canada’s air marshall program). However, there was a broad consensus among witnesses that if consideration is given to expanding its use, behavioural analysis should be thoroughly reviewed in order to determine whether its benefits outweigh the risks it poses to individual rights.
- The value of Canada’s air marshall program is impossible to quantify, but it may provide another layer of protection, particularly in relation to high-risk flights.
- The “no-fly list” program has not proven to be effective.
- There is no coordinated, system-wide risk management strategy among stakeholders in Canadian aviation security, which may allow significant risks in civil aviation to go unnoticed.

TERRORIST FINANCING

- Canada’s current anti-terrorist financing model, which was created on the basis of its existing anti-money laundering model, is not well-suited to capture terrorist financing transactions.
- Canada must comply with a series of international obligations and requirements in terms of its anti-terrorist financing programs and activities. For the most part, Canada is in compliance with those requirements but as is often the case in such matters, this is a continuing effort and there is still room for improvement.
- Up until at least very recently, the level of resources dedicated to anti-terrorist financing measures was inadequate. Resource levels in all concerned agencies or departments should be monitored and modified as needed on a regular basis.

- The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Canada Revenue Agency (CRA) are not adequately integrated into the intelligence cycle to effectively detect terrorist financing or to provide the best financial intelligence to CSIS and the RCMP.
- As of the Commission hearings, the CRA had not revoked or deregistered any charitable registrations on grounds of terrorism financing.
- It is not clear that all relevant federal, provincial and municipal authorities have the same appreciation of the risks posed by terrorism financing. There is definite room for improvement in terms of intergovernmental cooperation and efforts to combat that phenomenon.